JK 5/26/01

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1803	((713/163) or (713/180) or (380/28) or (380/30) or (380/33)).CCLS.	USPAT	OR	OFF	2006/05/26 13:30
L2	26	1 and (@pd > "20060428")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/05/26 12:51
L3	16	((prime adj number) and (random adj (number value)) and (encrypt$3 encipher$4) and integer and (decrypt$3 decipher$4)).clm.	US-PGPUB	OR	ON	2006/05/26 13:37
L5	1	(absolute adj public adj key) with encrypt$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/05/26 13:39
L6	4	((private adj key with compromise) and public adj key).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/05/26 13:40
S1	2	(("6081598") or ("4405829")).PN.	USPAT	OR	OFF	2006/05/26 12:51
S2	2	delsarte.in.	USPAT	OR	OFF	2004/12/03 12:45
S3	21	delaurentis.in.	USPAT	OR	OFF	2004/12/03 13:15
S4	389528	blinding factors	USPAT	OR	OFF	2004/12/03 13:15
S5	11	(blinding adj factors) and rsa	USPAT	OR	OFF	2006/04/28 12:34
S6	2	(blinding adj factors) and (euler adj totient adj function)	USPAT	OR	OFF	2004/12/03 14:55
S7	0	(blinding adj factor) and (euler adj totient adj function)	USPAT	OR	OFF	2004/12/03 14:55
S8	0	(blinding adj factor) and (euler adj totient adj function)	US-PGPUB; USPAT; EPO	OR	OFF	2004/12/03 14:55
S9	4	(blinding adj factors) and (euler adj totient adj function)	US-PGPUB; USPAT; EPO	OR	OFF	2004/12/03 15:11
S10	67	rsa and (secret adj sharing)	USPAT	OR	OFF	2004/12/03 15:21

EAST Search History

S11	0	cheman-shaik.in.	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2004/12/03 15:21
S12	7	(euler totient) same (blind blinding)	USPAT	OR	OFF	2004/12/03 16:13
S13	8	(euler totient) same (blind blinding)	USPAT; USOCR; EPO; JPO	OR	OFF	2004/12/03 17:35
S14	0	confidentiality and (private-to-public) and rsa	USPAT	OR	OFF	2004/12/03 17:35
S15	0	confidentiality and (private-to-public)	USPAT	OR	OFF	2004/12/03 17:36
S16	30	rsa and totient	USPAT	OR	OFF	2004/12/03 17:44
S17	0	routing adj different adj encrypted	USPAT	OR	OFF	2004/12/03 17:47
S18	0	rsa and euler and (blind adj key)	USPAT	OR	OFF	2004/12/03 17:47
S19	0	rsa and (blind adj key)	USPAT	OR	OFF	2004/12/03 17:47
S20	75	(713/163).CCLS.	USPAT	OR	OFF	2004/12/13 16:30
S21	14	S20 and rsa	USPAT	OR	OFF	2004/12/13 16:33
S22	608	380/277	USPAT	OR	OFF	2004/12/13 16:34
S23	400	(380/277).CCLS.	USPAT	OR	OFF	2004/12/13 16:34
S24	120	S23 and rsa	USPAT	OR	OFF	2004/12/13 16:34
S25	10	S23 and (blind blinding)	USPAT	OR	OFF	2004/12/13 16:36
S26	168	(380/239).CCLS.	USPAT	OR	OFF	2004/12/13 16:37
S27	25	S26 and rsa	USPAT	OR	OFF	2004/12/13 16:42
S28	174	(380/33).CCLS.	USPAT	OR	OFF	2004/12/13 16:42
S29	7	S28 and rsa	USPAT	OR	OFF	2004/12/13 16:44
S30	197	(713/180).CCLS.	USPAT	OR	OFF	2004/12/13 16:44
S31	116	S30 and rsa	USPAT	OR	OFF	2004/12/13 16:55
S32	1	"weak privacy protocol"	USPAT	OR	OFF	2004/12/15 09:10
S33	1	"weak privacy protocol"	US-PGPUB; USPAT; USOCR; EPO	OR	OFF	2004/12/15 09:10
S34	0	"G.J. Simmons"	US-PGPUB; USPAT; USOCR; EPO	OR	OFF	2004/12/15 09:10
S35	0	"G.J. Simmons$"	US-PGPUB; USPAT; USOCR; EPO	OR	OFF	2004/12/15 09:11

EAST Search History

S36	0	"G.J. Simmons"$	US-PGPUB; USPAT; USOCR; EPO	OR	OFF	2004/12/15 09:11
S37	0	$"G.J. Simmons"$	US-PGPUB; USPAT; USOCR; EPO	OR	OFF	2004/12/15 09:11
S38	0	"G.J." adj "Simmons"	US-PGPUB; USPAT; USOCR; EPO	OR	OFF	2004/12/15 09:12
S39	1	common adj modulus adj protocol adj failure	USPAT	OR	OFF	2004/12/15 09:12
S40	0	common adj modulus adj failure	USPAT	OR	OFF	2004/12/15 09:12
S41	1	modulus adj protocol adj failure	USPAT	OR	OFF	2004/12/15 09:12
S42	36	modulus adj failure	USPAT	OR	OFF	2004/12/15 09:14
S43	0	rsa and (blind adj key adj encryption)	USPAT	OR	OFF	2004/12/15 09:14
S44	0	rsa and (blind-key adj encryption)	USPAT	OR	OFF	2004/12/15 09:14
S45	1	rsa and (blind-key adj encryption)	US-PGPUB; USPAT	OR	OFF	2004/12/15 09:20
S46	18	(common adj factor) same phi	USPAT	OR	OFF	2004/12/15 09:20
S47	10	(common adj factor) same phi and rsa	USPAT	OR	OFF	2004/12/15 09:29
S48	0	(relative adj composite-key adj encryption)	USPAT	OR	OFF	2004/12/15 09:29
S49	0	(relative adj composite-key)	USPAT	OR	OFF	2004/12/15 09:29
S50	0	direct adj source adj routing	USPAT	OR	OFF	2004/12/16 12:18
S51	509	source adj routing	USPAT	OR	OFF	2004/12/16 12:18
S52	15	S51 and rsa	USPAT	OR	OFF	2004/12/16 12:20
S53	660	(380/28).CCLS.	USPAT	OR	OFF	2004/12/16 13:24
S54	200	S53 and rsa	USPAT	OR	OFF	2004/12/16 13:24
S55	779	(380/30).CCLS.	USPAT	OR	OFF	2004/12/16 13:24
S56	475	S55 and rsa	USPAT	OR	OFF	2004/12/16 13:24
S57	12	S54 and S56 and (blind$)	USPAT	OR	OFF	2004/12/16 13:24
S58	1	("5892900").PN.	USPAT	OR	OFF	2004/12/16 14:30
S59	1	("6338141").PN.	USPAT	OR	OFF	2004/12/17 09:56
S60	1777	((713/163) or (713/180) or (380/28) or (380/30) or (380/33)).CCLS.	USPAT	OR	OFF	2006/04/28 10:52

EAST Search History

S61	205	S60 and (@pd > "20041216")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/04/28 10:52
S62	0	blind adj exponent	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/04/28 12:35
S63	3	blinding adj exponent	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/04/28 12:43
S64	180	blind$4 same (add$3) same random$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/04/28 12:44
S65	20	blind$4 same (add$3) same random$3 same key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/04/28 12:56
S66	6	add with random adj number with (public adj key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/04/28 12:57

12 5/26/06

Terms used **blind key encryption blinding random** Found **249** of **176,279**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 A resolution strategy for verifying cryptographic protocols with CBC encryption and blind signatures
Véronique Cortier, Michael Rusinowitch, Eugen Z□linescu
July 2005 **Proceedings of the 7th ACM SIGPLAN international conference on Principles and practice of declarative programming PPDP '05**
Publisher: ACM Press
Full text available: pdf(214.71 KB) Additional Information: full citation, abstract, references, index terms

Formal methods have proved to be very useful for analyzing cryptographic protocols. However, most existing techniques apply to the case of abstract encryption schemes and pairing. In this paper, we consider more complex, less studied cryptographic primitives like CBC encryption and blind signatures. This leads us to introduce a new fragment of Horn clauses. We show decidability of this fragment using a combination of several resolution strategies.As a consequence, we obtain a new decidability re ...

Keywords: cryptographic protocols, horn clauses, resolution strategies, verification

2 Agents, interactions, mobility and systems: Blinded-key signatures: securing private keys embedded in mobile agents
Lucas C. Ferreira, Ricardo Dahab
March 2002 **Proceedings of the 2002 ACM symposium on Applied computing**
Publisher: ACM Press
Full text available: pdf(442.06 KB) Additional Information: full citation, abstract, references, index terms

We present a new cryptographic primitive, the *blinded-key signature,* which allows the inclusion of private keys in autonomous mobile agents. This novel approach can be applied to many well-known digital signature schemes, such as RSA and ElGammal.

Keywords: cryptography, digital signatures, mobile agents, security

3 Multi-agent systems and social behavior: Blind sales in electronic commerce
E. Aïmeur, G. Brassard, F. S. Mani Onana
March 2004 **Pr ceedings f the 6th internati nal c nference n Electr nic c mmerce ICEC '04**
Publisher: ACM Press
Full text available: pdf(330.05 KB) Additional Information: full citation, abstract, references

We start with the usual paradigm in electronic commerce: a consumer who wants to buy from a merchant. However, both parties wish to enjoy maximal privacy. In addition to remaining anonymous, the consumer wants to hide her browsing pattern and even the identification of the product she may decide to buy. Nevertheless, she wants to be able to negotiate the price, pay, receive the product and even enjoy maintenance on it. On the other hand, the merchant wants to leak as little information as possib ...

Keywords: CAPTCHA, anonymous surfing, cryptography, customer buying behaviour, electronic commerce, oblivious transfer, private information retrieval

4 Revokable and versatile electronic money (extended abstract)

Markus Jakobsson, Moti Yung

January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

5 Strength of two data encryption standard implementations under timing attacks

Alejandro Hevia, Marcos Kiwi

November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4

Publisher: ACM Press

Full text available: pdf(183.73 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study the vulnerability of two implementations of the Data Encryption Standard (DES) cryptosystem under a timing attack. A timing attack is a method, recently proposed by Paul Kocher, that is designed to break cryptographic systems. It exploits the engineering aspects involved in the implementation of cryptosystems and might succeed even against cryptosys-tems that remain impervious to sophisticated cryptanalytic techniques. A timing attack is, essentially, a way of obtaining some users ...

Keywords: cryptanalysis, cryptography, data encryption standard, timing attack

6 Secure key issuing in ID-based cryptography

Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang, Seungjae Yoo

January 2004 **Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation - Volume 32 CRPIT '04**

Publisher: Australian Computer Society, Inc.

Full text available: pdf(177.95 KB) Additional Information: full citation, abstract, references

ID-based cryptosystems have many advantages over PKI based cryptosystems in key distribution, but they also have an inherent drawback of key escrow problem, i.e. users' private keys are known to the key generation center (KGC). Therefore secure key issuing (SKI) is an important issue in ID-based cryptography. In multiple authority approach (Boneh & Franklin 2001, Chen et al. 2002), key generation function is distributed to multiple authorities. Keeping key privacy using user-chosen secret inform ...

Keyw rds: ID-based cryptography, bilinear pairing, blinding, key generation center (KGC), key privacy authority (KPA), secure key issuing (SKI)

7 A survey of key management for secure group communication

Sandro Rafaeli, David Hutchison

September 2003 **ACM C mputing Surveys (CSUR)**, Volume 35 Issue 3

Publisher: ACM Press

Full text available: pdf(346.27 KB) Additional Information: full citation, abstract, references, citings, index terms

Group communication can benefit from IP multicast to achieve scalable exchange of messages. However, there is a challenge of effectively controlling access to the transmitted data. IP multicast by itself does not provide any mechanisms for preventing nongroup members to have access to the group communication. Although encryption can be used to protect messages exchanged among group members, distributing the cryptographic keys becomes an issue. Researchers have proposed several different approach ...

Keywords: Group Key Distribution, Multicast Security

8 On the performance of group key agreement protocols

Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, Gene Tsudik

August 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 3

Publisher: ACM Press

Full text available: pdf(469.07 KB) Additional Information: full citation, abstract, references, index terms

Group key agreement is a fundamental building block for secure peer group communication systems. Several group key management techniques were proposed in the last decade, all assuming the existence of an underlying group communication infrastructure to provide reliable and ordered message delivery as well as group membership information. Despite analysis, implementation, and deployment of some of these techniques, the actual costs associated with group key management have been poorly understood ...

Keywords: Group Communication, Group Key Management, Peer Groups, Secure Communication

9 Simple and fault-tolerant key agreement for dynamic collaborative groups

Yongdae Kim, Adrian Perrig, Gene Tsudik

November 2000 **Proceedings of the 7th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(319.01 KB) Additional Information: full citation, references, citings, index terms

10 Unlinkable serial transactions: protocols and applications

Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag

November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4

Publisher: ACM Press

Full text available: pdf(184.87 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned

use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

Keyw rds: anoymity, blinding, cryptographic protocols, unlinkable serial transactions

11 Practical multi-candidate election system

Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, Guillaume Poupard
August 2001 **Proceedings of the twentieth annual ACM symposium on Principles of distributed computing**
Publisher: ACM Press

Full text available: pdf(898.50 KB) Additional Information: full citation, abstract, references, citings, index terms

The aim of electronic voting schemes is to provide a set of protocols that allow voters to cast ballots while a group of authorities collect the votes and output the final tally. In this paper we describe a practical multi-candidate election scheme that guarantees privacy of voters, public verifiability, and robustness against a coalition of malicious authorities. Furthermore, we address the problem of receipt-freeness and incoercibility of voters. Our new scheme is based on the Paillier cryp ...

12 Tree-based group key agreement

Yongdae Kim, Adrian Perrig, Gene Tsudik
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press

Full text available: pdf(573.70 KB) Additional Information: full citation, abstract, references, citings, index terms

Secure and reliable group communication is an active area of research. Its popularity is fueled by the growing importance of group-oriented and collaborative applications. The central research challenge is secure and efficient group key management. While centralized methods are often appropriate for key distribution in large multicast-style groups, many collaborative group settings require distributed key agreement techniques. This work investigates a novel group key agreement approach which ble ...

Keywords: communication complexity, cryptographic protocols, group communication, group key agreement, security

13 Physical privacy: Privacy management for portable recording devices

J. Alex Halderman, Brent Waters, Edward W. Felten
October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic society**
Publisher: ACM Press

Full text available: pdf(321.69 KB) Additional Information: full citation, abstract, references, index terms

The growing popularity of inexpensive, portable recording devices, such as cellular phone cameras and compact digital audio recorders, presents a significant new threat to privacy. We propose a set of technologies that can be integrated into recording devices to provide stronger, more accurately targeted privacy protections than other legal and technical measures now under consideration. Our design is based on an informed consent principle, which it supports by the use of novel devices and pr ...

Keyw rds: camera phones, privacy, recording devices

14

Short papers: Specifying electronic voting protocols in typed MSR
Theodoros Balopoulos, Stefanos Gritzalis, Sokratis K. Katsikas
November 2005 **Pr ceedings f the 2005 ACM w rkshop n Privacy in the electr nic s ciety WPES '05**
Publisher: ACM Press
Full text available: pdf(141.00 KB) Additional Information: full citation, abstract, references, index terms

Electronic voting, as well as other privacy-preserving protocols, use special cryptographic primitives and techniques that are not widely used in other types of protocols, e.g. in authentication protocols. These include blind signatures, commitments, zero-knowledge proofs, mixes and homomorphic encryption. Furthermore, typical formalizations of the Dolev-Yao intruder's capabilities do not take into account these primitives and techniques, nor do they consider some types of attacks that e-voting ...

Keywords: Dolev-Yao intruder, electronic voting, privacy, security protocols, specification, typed MSR

15 A secure and private system for subscription-based remote services
Pino Persiano, Ivan Visconti
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4
Publisher: ACM Press
Full text available: pdf(241.65 KB) Additional Information: full citation, abstract, references, index terms

In this paper we study privacy issues regarding the use of the SSL/TLS protocol and X.509 certificates. Our main attention is placed on subscription-based remote services (e.g., subscription to newspapers and databases) where the service manager charges a flat fee for a period of time independent of the actual number of times the service is requested.We start by pointing out that restricting the access to such services by using X.509 certificates and the SSL/TLS protocol, while preserving the in ...

Keywords: Access control, anonymity, cryptographic algorithms and protocols, privacy, world-wide web

16 Strong loss tolerance of electronic coin systems
Birgit Pfitzmann, Michael Waidner
May 1997 **ACM Transactions on Computer Systems (TOCS)**, Volume 15 Issue 2
Publisher: ACM Press
Full text available: pdf(267.29 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Untraceable electronic cash means prepaid digital payment systems, usually with offline payments, that protect user privacy. Such systems have recently been given considerable attention by both theory and development projects. However, in most current schemes, loss of a user device containing electronic cash implies a loss of money, just as with real cash. In comparison with credit schemes, this is considered a serious shortcoming. This article shows how untraceable electronic cash can be m ...

Keywords: Byzantine faults, electronic cash, payment systems, privacy

17 Ad hoc networks: On the security of group communication schemes based on symmetric key cryptosystems
Shouhuai Xu
November 2005 **Pr ceedings f the 3rd ACM w rksh p on Security f ad h c and**

sens r netw rks SASN '05

Publisher: ACM Press

Full text available: pdf(259.19 KB) Additional Information: full citation, abstract, references, index terms

Many emerging applications in both wired and wireless networks, such as information dissemination and distributed collaboration in an adversarial environment, need support of secure group communications. There have been many such schemes in the setting of wired networks. These schemes can be directly adopted in, or appropriately adapted to, the setting of wireless networks such as mobile ad hoc networks (MANETs) and sensor networks. In this paper we show that the popular group communication sche ...

Keywords: backward-security, broadcast encryption, forward-security, group communication, key management, security

18 The Ω key management service

Michael K. Reiter, Matthew K. Franklin, John B. Lacy, Rebecca N. Wright

January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(1.37 MB) Additional Information: full citation, references, citings, index terms

19 The design and implementation of a private message service for mobile computers

David A. Cooper, Kenneth P. Birman

August 1995 **Wireless Networks**, Volume 1 Issue 3

Publisher: Kluwer Academic Publishers

Full text available: pdf(1.35 MB) Additional Information: full citation, abstract, references

Even as wireless networks create the potential for access to information from mobile platforms, they pose a problem for privacy. In order to retrieve messages, users must periodically poll the network. The information that the user must give to the network could potentially be used to track that user. However, the movements of the user can also be used to hide the user's location if the protocols for sending and retrieving messages are carefully designed. We have developed a replicated memo ...

20 A secure marketplace for mobile Java agents

Kay Neuenhofen, Matthew Thompson

May 1998 **Proceedings of the second international conference on Autonomous agents**

Publisher: ACM Press

Full text available: pdf(889.69 KB) Additional Information: full citation, references, citings, index terms

Keywords: agent architectures, mobile agents, security

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next